产品简介

赛门铁克端点安全

实施协调一致的端点安全策略比以往任何时候都重要

介绍

端点是网络攻击者的主要目标。随着攻击成功的后果和造成的损失越来越大，许多公司试图通过添加多个端点保护来加强他们的整体防御。产品。不幸的是，这种方法削弱了组织的安全态势。

Ponemon研究所发现，企业平均安装了七种不同的端点代理来支持IT管理和安全。[1] 每个代理都是独立运行的，有自己的控制台和一套规则。和策略--所有这些都必须进行配置、推出、管理和维护。除了造成更多的IT开销和成本外，多种产品还引入了防御漏洞和错误，增加了错过威胁的机会。

预防很重要，因为全球网络威胁比以往任何时候都更加咄咄逼人，而且会对企业产生惊人的影响。在您阅读本产品简介的时间内，整个企业可能会受到损害。据报道，NotPetya攻击使全球最大的航运公司之一陷入瘫痪。与其他数千家企业一样，在短短7分钟内，就有数千家公司被攻击[2]。由于现代攻击的检测和反应窗口非常短，因此尽早预防攻击至关重要。投資於事故回應，对于建立坚固的安全態勢以防止未來的攻擊也很重要。有了賽門鐵克，您就可以杜絕危害。既然您可以同时拥有最好的安全性和最简单的操作，为什么要在两者之间做出选择呢？

图1：赛门铁克端点安全完整版

1：《2017年端点安全风险状况》，Ponemon Institute LLC，2017年11月。

Symantec Endpoint Security Complete的主要功能

- 保护所有端点：笔记本电脑、台式机、平板电脑、移动设备和服务器。
- 用于减少攻击面、攻击预防、漏洞预防和端点检测与响应（EDR）的单一代理。
- 具有实时威胁可视性的单一控制台
- 灵活的部署：内部、云管理和混合模式。
- 活动目录安全
- 行为隔离和应用控制能力
- 人工智能（AI）指导下的安全管理
- 目标攻击分析和威胁猎人
- 全球情报网（GIN）是全球最大的情报网之一，提供实时威胁信息、威胁分析、内容分类和
全面的威胁拦截数据
- 通过赛门铁克ICDx与第三方应用程序（包括Microsoft Graph、Open C2和其他赛门铁克解决方案）集成。

企业版主要功能

- 保护笔记本电脑、台式机、手机和平板电脑。
- 端点安全的单一代理
- 具有实时威胁可视性的单一控制台
- 灵活的部署：内部、云管理和混合模式。
- 人工智能（AI）指导下的安全管理
- 全球最大的情报网络之一，提供实时威胁信息。
- 通过赛门铁克集成网络防御交换(ICDx)与第三方应用程序(如Microsoft Graph、Open C2)和其他赛门铁克解决方案集成。

解决方案概述

赛门铁克端点安全完整版提供了全球最全面、最集成的端点安全平台。作为一个现场　应对针对您的端点的所有高级威胁。

为您的组织提供无与伦比的端点安全
赛门铁克端点安全为您的企业在端点为传统和移动设备提供最好的安全防护，跨越三个攻击阶段--攻击前、攻击和攻击后，强调整个攻击链的预防，以实现快速遏制。主动减少攻击面和创新的攻击预防技术，为最难发现的威胁提供了最强的防御，这些威胁依靠隐蔽的恶意软件、凭证窃取、无文件和"靠天吃饭"的攻击方式。赛门铁克还能在外泄发生之前防止全面的漏洞。复杂的攻击分析、行为取证、自动调查演习以及业界首创的横向移动和凭证窃取预防，可提供精确的攻击。
检测和主动性威胁猎取，以遏制攻击者并实时解决持续威胁。

减少攻击面

赛门铁克提供主动式**端点防御**，以先**进**的政策控制和技術**为**基**础**的**预**攻**击**面**缩减**功能，持续**扫**描**应**用程式、活动**目录**和设备的漏洞和**错**誤配置。有了攻击面减少防御功能，许多攻击者的策略和技术就无法在您的端点资产上得到利用。

- 违规评估持续探测活动目录的域错误配置、漏洞和持久性，使用攻击模拟来识别风险，允许立即缓解，并提供补救措施的规范性建议。
- 设备控制对连接到客户端计算机的不同类型的设备（如USB、红外和火线设备）指定阻止或允许策略，以降低威胁和渗透的风险。
- 应用程序控制评估应用程序的风险及其漏洞，只允许已知的良好应用程序运行。
- 行为隔离限制了受信任应用的异常和风险行为，对操作影响最小。
- 漏洞修复[3]通过提供漏洞及其相关风险的可视性和情报，增强安全态势。发现的漏洞将根据CVSS（通用漏洞评分系统）的严重性和受影响设备的数量进行排名，以确保首先修复最严重的威胁。

3：仅在Win 10、Win 10的S模式、iOS和Android设备上支持。

攻击预防

赛门铁克多层攻击防御可立即有效地防范基于文件和无文件的攻击载体和方法。其机器学习和人工智能使用先进的设备和基于云的检测方案来识别跨设备类型、操作系统和应用程序的不断变化的威胁。攻击会被实时阻止，因此端点可以保持完整性，避免负面影响。

- 恶意软件预防结合了对新的和不断发展的威胁的执行前检测和阻断（高级机器学习、检测隐藏在自定义打包程序中的恶意软件的沙箱和可疑文件行为监控和阻断），以及基于签名的方法（文件和网站信誉分析和恶意软件扫描）。
- Exploit Prevention 阻止基于内存的零日漏洞利用流行软件中的漏洞。
- 强化保护可单独对检测和阻断级别进行细微调整，以优化保护，并增强对可疑文件的可见性。
- 网络连接安全可识别流氓Wi-Fi网络，利用热点信誉技术，并提供策略驱动的VPN，以保护网络连接并支持合规性。

违规预防

赛门铁克的预防方法需要在攻击者有任何机会在网络上持续存在之前，尽早在端点遏制攻击者。各种人工智能驱动的欺骗和入侵防御技术共同合作，在端点入侵之前和之后立即阻止网络持续存在--在全面入侵发生之前。

- 入侵防御和防火墙使用规则和策略阻止已知的网络和基于浏览器的恶意软件攻击，并通过自动域名IP地址黑名单防止命令和控制设置。
- 欺骗使用引诱和诱饵（假文件、凭证、网络共享、缓存条目、Web请求和端点）来暴露、确定攻击者的意图和战术，并通过早期可见性来延迟攻击者。
- 活动目录安全通过使用无限制的混淆(指假资产和凭证创建)控制攻击者从终端对组织的活动目录资源的感知来防御横向移动和域管理员凭证盗窃的主要攻击面。通过混淆，攻击者在活动目录的感知上与*假*资产交互或尝试使用域管理员凭证时，就会泄露自己。
- 自动管理策略，基于先进的AI和ML，独特地结合了妥协和历史异常的指标，以持续调整端点策略阈值或规则，并使其保持最新状态，并与您的组织的当前风险状况保持一致。

泄密后的应对和补救措施

赛门铁克将端点检测和响应(EDR)技术与无与伦比的安全运营中心(SOC)分析师专业技术相结合，为您提供必要的工具，以快速关闭端点事件并将攻击影响降至最低。在涵盖传统和现代端点的单一代理架构中，集成的EDR功能可精确检测高级攻击，提供实时分析，并使您能够主动猎取威胁并进行取证调查和修复。

- 行为取证提供了记录和分析端点行为的能力，以识别可能将合法应用用于恶意目的的高级攻击技术。这些数据经过MITRE ATT&CK框架的丰富，有助于指导事件响应者进行调查。
- 赛门铁克EDR中提供了先进的威胁猎取工具，包括内置的游戏手册，其中囊括了熟练的威胁猎取者和异常行为检测的最佳实践。事故响应人员可以在整个企业内猎取IOC，包括直接查询端点。
- 集成响应在端点上直接采取行动，通过检索文件、删除文件、隔离端点和列入黑名单进行补救。赛门铁克EDR支持将已识别的可疑文件自动提交到沙箱中，以进行完整的恶意软件分析，包括暴露具有虚拟机感知能力的恶意软件。

泄密后的应对和补救措施（续）。

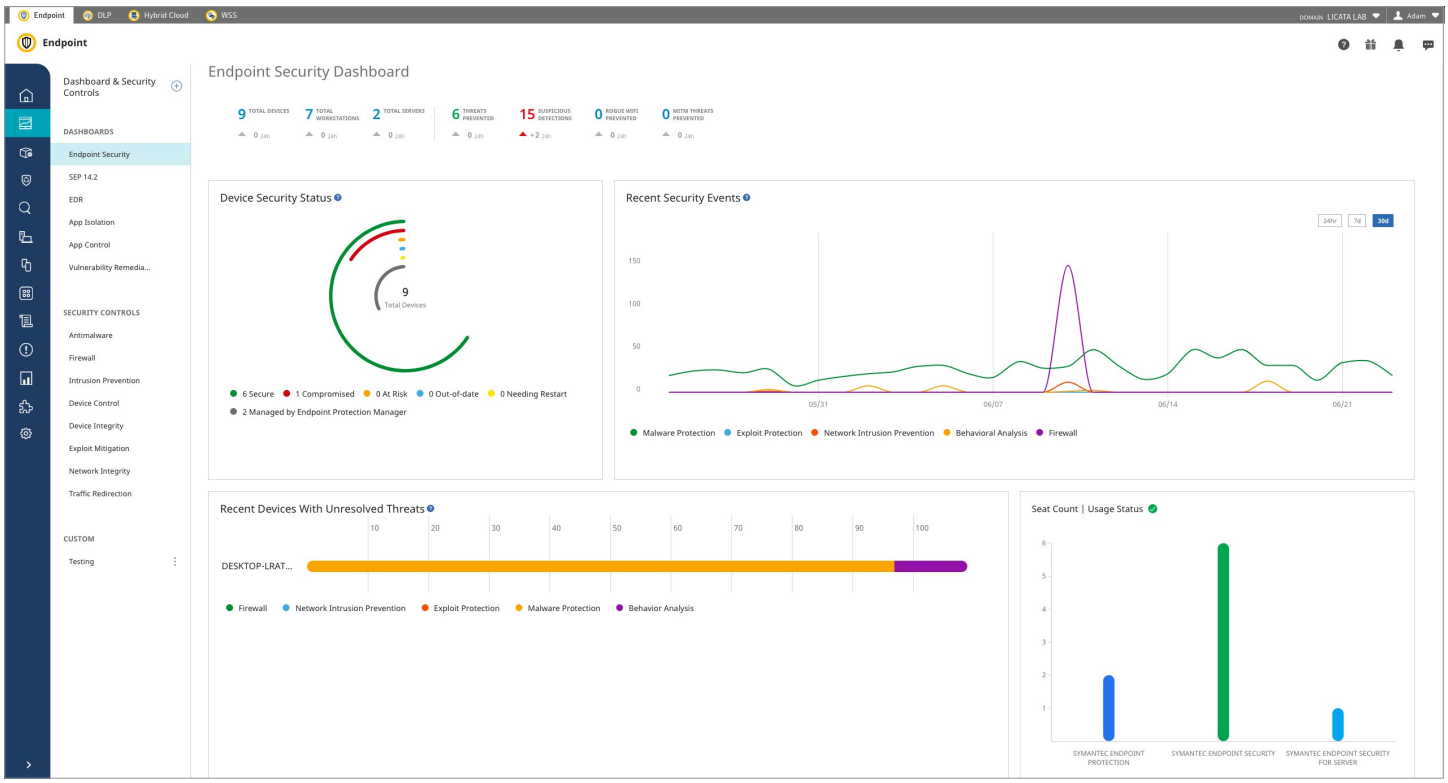
- Threat Hunter可猎取高保真事件，并结合先进的机器学习和专家SOC分析师的力量，发现对手使用的工具、战术和程序。它确保通过相关背景快速识别关键攻击。此外，它还提供对赛门铁克全球安全数据的直观访问，以增强您团队的威胁猎取工作。
- 快速响应将补救威胁和实时响应攻击者的时间降到最低。内置的工具和游戏手册通过隔离攻击者和提供对端点的交互式访问来控制威胁。

轻松保护您的动态端点环境

单一代理堆栈减少了您的端点安全足迹，同时整合（和协调）了最佳可用的预防、检测和响应技术。从一个基于云的管理系统（Integrated Cyber Defense Manager）管理一切，最大限度地减少配置、推出、管理和维护安全态势所需的时间、资源和精力。您只需点击一两下就可以访问所需的一切，提高管理员的工作效率，并加快响应时间，以快速关闭安全事件。

- AI引导的安全管理更准确地更新策略，更少的错误配置，提高你的安全防护。
- 简化的工作流程确保了一切工作都能协调一致，以提高性能、效率和生产力。
- 情境感知建议通过消除常规任务并做出更好的决策，帮助实现最佳性能。
- 自主安全管理不断从管理员和用户行为中学习，以改进威胁评估、调整响应，并加强您的整体安全态势。

图2：端点用户界面



利用广泛的赛门铁克产品组合和第三方集成降低复杂性

赛门铁克端点安全是一个基础性的解决方案，可促进整合，使IT安全团队能够检测到其网络中任何地方的威胁，并通过协调响应来应对这些威胁。赛门铁克端点安全解决方案与其他赛门铁克解决方案一起工作，并通过专用

应用程序和发布的API与第三方产品一起工作，以加强您的安全态势。没有其他厂商提供整合式解决方案，可在端點上协调因检测到网络和电子邮件安全网关上的威胁而引发的回应（黑名单和修复）。具体的集成包括：

- 赛门铁克网络安全服务。使用PAC文件将漫游的赛门铁克端点安全用户的网络流量重定向到赛门铁克网络安全服务和赛门铁克CASB。
- 赛门铁克网络网关。可编程的REST API使得与内部网络安全基础设施的集成成为可能。
- 赛门铁克验证和ID保护。多因素验证，包括PIV/CAC智能卡到Symantec Endpoint Security on-prem和基于云的管理控制台。
- 赛门铁克内容分析。利用动态预置沙箱和额外的威胁引擎，进一步分析赛门铁克端点安全系统发送的可疑文件。
- 赛门铁克数据丢失防护。通过向DLP提供可疑应用的实时威胁情报，防止敏感信息的数据外泄。

图3：赛门铁克端点安全

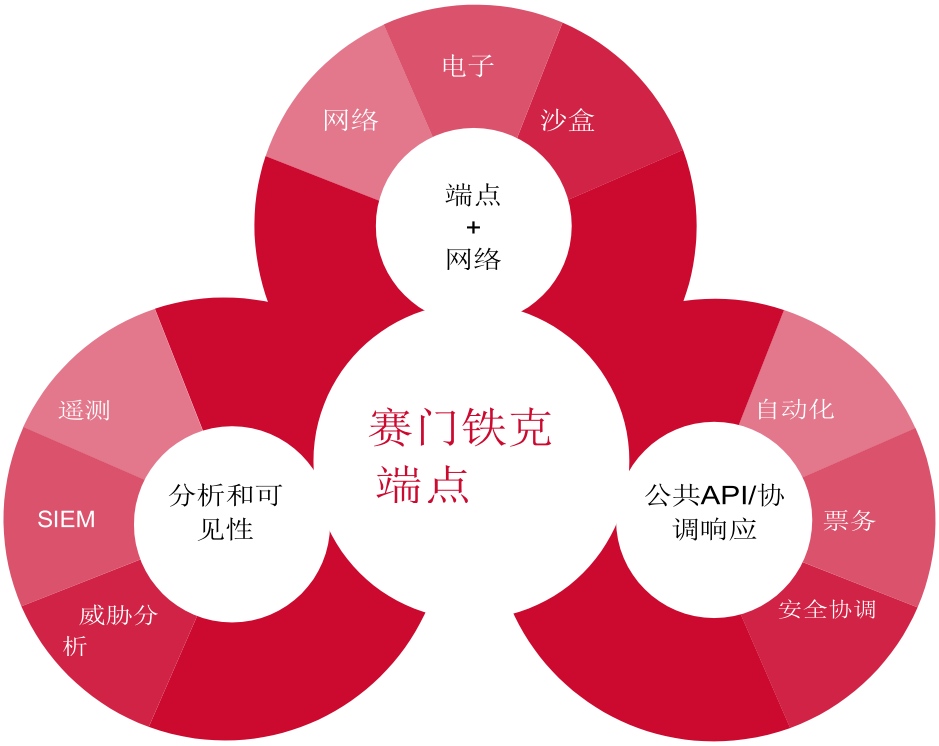


Figure 4: License Options

Features

	SEP	SES ENTERPRISE	SES COMPLETE
	Industry standard in Endpoint Protection. 5 years running as #1 Protection and now also #1 Performance by AV Test.	Extends SEP to all OSs and all devices including mobile. Offers cloud management.	Adds advanced protection, EDR, threat hunting, and other technologies for complete protection.
MANAGEMENT OPTIONS	On-Premises	On-Premises, Cloud, Hybrid	
AGENTS REQUIRED	SINGLE SYMANTEC AGENT		
DEVICE COVERAGE Corporate Owned, BYOD, UYOD	Laptop, Desktop, Server	Mobile, Tablet, Laptop, Desktop, Server	
OS COVERAGE	Windows, macOS, Linux	Windows (including S Mode and Arm), macOS, iOS, Linux, Android	

Protection Technologies

	SEP	SES ENTERPRISE	SES COMPLETE
ATTACK PREVENTION			
INDUSTRY BEST ATTACK PREVENTION	✓	✓	✓
MOBILE THREAT DEFENSE		✓	✓
SECURE NETWORK CONNECTION		✓	✓
ATTACK SURFACE REDUCTION			
BREACH ASSESSMENT			✓
BEHAVIORAL ISOLATION			✓
APPLICATION CONTROL			✓
DEVICE CONTROL	✓	✓	✓
BREACH PREVENTION ...			
INTRUSION PREVENTION	✓	✓	✓
FIREWALL	✓	✓	✓

	SEP	SES ENTERPRISE	SES COMPLETE
... BREACH PREVENTION			
DECEPTION	✓	✓	✓
ACTIVE DIRECTORY SECURITY			✓
RESPONSE AND REMEDIATION			
ENDPOINT DETECTION AND RESPONSE			✓
TARGETED ATTACK CLOUD ANALYTICS			✓
BEHAVIORAL FORENSICS			✓
THREAT HUNTER			✓
RAPID RESPONSE			✓
IT OPERATIONS			
DISCOVER & DEPLOY	✓	✓	✓
HOST INTEGRITY CHECKS	✓	✓	✓

Symantec™
A Division of Broadcom

For product information, visit our website at: go.broadcom.com/ses

SED-EPS-PB101 June 25, 2020